AMENDMENTS TO THE CLAIMS

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Canceled)

2. (Canceled)

3. (Canceled)

4. (Canceled)

5. (Canceled)

6. (Currently Amended) A method for sending a message, said method comprising the steps of:

   a) generating by a sender a password P;

   b) sending the password P to a message recipient over a first channel;

   c) generating authentication information by the sender for server authentication of the message recipient, wherein the authentication information is dependent on knowing the password P;

   d) generating by the sender a random number as an initialization vector IV4;

   e) generating by the sender a private key PK as H(IV4 | P), where P is a password known to a message recipient, H( ) is an agreed upon hashing algorithm and (|) is a message concatenation;

   f) generating by the sender an encryption ENC = E(M | H(M), PK), where E is a predetermined symmetric key encryption algorithm, M is the message;

   g) sending the authentication information and (IV4, ENC) from the sender to the server over a second channel;

   h) authenticating the message recipient over a third channel using the authentication information to verify that the message recipient knows the password P; wherein the authentication information comprises:

h-1) the authentication response AR as E(ACNST2, ARK) generated by the message recipient, where ACNST2 is a predetermined constant;

h-2) the authentication response key ARK as H(IV2 | IV3 | AS), where IV2 is a second random number (as a second initialization vector) generated by the server and IV3 is a third random number (as a third initialization vector) generated by the message recipient;

h~3) the authentication string AS is as E(ACNST1, PKAK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm and AK is an authentication key derived from the password P.

i) sending ENC from the server to the message recipient over the third channel only when the message recipient has been authenticated by the server.

7. (Original) A method as described in claim 6 comprising the further step of receiving authentication of said message recipient prior to sending (IV4, ENC).

8. (Currently Amended) A method as described in claim 6 wherein step c) further comprises the steps of:

i) generating by the sender a first random number as a first initialization vector IV1;

ii) generating by the sender H(IV1 | P) as an authentication key AK;

iii) generating by the sender an authentication string AS as E(ACNST1, AK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm;

and wherein step g) further comprises the steps of sending IV1 and AS to the server over the second channel:

and wherein step h) further comprises the steps of:

iv) sending from the server said vectors IV1 and IV2 to said message recipient over the third channel;

v) regenerating by said message recipient the authentication key AK;

vi) regenerating by said message recipient the authentication string AS;

vii) sending from said message recipient to the server IV3 and AR;

vii) regenerating by the server the authentication response key ARK as H(IV2 | V3 | AS);

ix) computing by the server a decryption D(AR, ARK), where D is a symmetric decryption algorithm corresponding to E; and

x) authenticating said message recipient only if D(AR, ARK) = ACNST2, where ACNST2 is a second predetermined constant;

and wherein step i) comprises the steps of:

xi) generating D(ENC, PK) = (M | H(M)), where D is a symmetric key decryption algorithm corresponding to E;

xii) calculating H(M) from said value of M generated in step c; and

xiii) accepting said generated value of M only if said calculated value of H(M) equals said value of H(M) generated in step c).

9. (Canceled)

10. (Original) A method as described in claim 6 where H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

11. (Original) A method as described in claim 10 where said encryption algorithm is expressed in less than 1000 bytes of code; whereby software comprising said algorithm can be quickly downloaded to a user's system.

12. (Original) A method as described in claim 11 where said encryption algorithm is an RC4 algorithm.

13. (Canceled)

14. (Canceled)

15. (Canceled)

16. (Canceled)

17. (Canceled)

18. (Canceled)

19. (Canceled)

20. (Canceled)

21. (Canceled)

22. (Canceled)

23. (Canceled)

24. (Canceled)

25. (Canceled)

26. (Canceled)

27. (Canceled)

28. (Canceled)

29. (Canceled)

30. (Canceled)

31. (Canceled)

32. (Canceled)

33. (Canceled)

34. (Canceled)

35. (Canceled)

36. (Canceled)

37. (Previously Presented) A system for sending a message, said system comprising:

a) means for generating by a sender a password P;

b) means for sending the password P to a message recipient over a first channel;

c) means for generating authentication information by the sender for server authentication of the message recipient, wherein the authentication information is dependent on knowing the password P;

d) means for generating by the sender a random number as an initialization vector IV4;

e) means for generating by the sender a private key PK as H(IV4 | P), where P is a password known to a message recipient, H( ) is an agreed upon hashing algorithm and (A|B) is a message concatenation;

f) means for generating by the sender an encryption ENC = E(M | H(M), PK), where E is a predetermined symmetric key encryption algorithm, M is the message;

g) means for sending the authentication information and (IV4, ENC) from the sender to the server over a second channel;

h) means for authenticating the message recipient over a third channel using the authentication information to verify that the message recipient knows the password P; wherein the authentication information comprises:

h-1) the authentication response AR as E(ACNST2, ARK) generated by the message recipient, where ACNST2 is a predetermined constant;

h-2) the authentication response key ARK as H(IV2 | IV3 | AS), where IV2 is a second random number (as a second initialization vector) generated by the server and IV3 is a third random number (as a third initialization vector) generated by the message recipient;

h-3) the authentication string AS is as E(ACNST1, PKAK), where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm and AK is an authentication key derived from the password P.

i) means for sending ENC from the server to the message recipient over the third channel only when the message recipient has been authenticated by the server.